ABSTRACT

A file that has been encrypted using a symmetric key and that has a corresponding access control entry with the symmetric key encrypted using the public key of a public/private key pair can be accessed. An encrypted key cache is also accessed to determine whether an access control entry to symmetric key mapping exists in the cache for the access control entry corresponding to the file. If such a mapping exists in the cache, then the mapped-to symmetric key is obtained form the cache, otherwise the encrypted symmetric key is decrypted using the private key of the public/private key pair. The encrypted key cache itself can also be encrypted and stored as an encrypted file.